Type of document	Policy
Title	Working With Student Records
Author	Head of Student Records
Document status	Approved
Next review date	December 2020
Security level	Public
Audience	Student Registry

CONTENTS

Working With Student Records

1. Introduction

This document is intended to provide a summary of best practice when working with student records. Following the guidelines within this document will assist colleagues in being compliant with Data Protection legislation and the reporting of data breaches.

This document may be relevant to colleagues across the collegiate University in demonstrating best practice that areas other than Student Registry may also wish to adopt.

2. Policy

The following points constitute Student Registry's policy on working with student records.

a. Desks

- Out of office hours, documents with identifiable student data, (for example, name, any other personal details, student number, etc.), must not be kept on desks or in desk filing trays.
- Documents currently being dealt with must be locked away overnight, either in lockable desk drawers or a shared lockable cupboard, with responsibility for locking of desk drawers on the individual, and locking of the shared cupboard on a defined individual. Keys should be kept in a secure place with no identifiable labelling as to the drawers'/cupboard's location.
- Staff will be responsible for collecting documents from printers, photocopiers, scanners, etc., to ensure that no documents with student data are left uncollected on or near devices.
- Computer screens must be locked whenever a desk is unattended (Ctrl+Alt+Delete "Lock" OR Win+L).

b. Digital filing

Digital folders on shared drives should only be accessible to those who have a need to see them. Access to shared folders should be managed centrally via IT Services, with restricted access granted by a small number of key authorisers. Access to shared drives should be reviewed regularly. Access can be maintained at https://help.it.ox.ac.uk/connect/requests

Agreed protocols should be in place for filing of documents containing student data, to ensure that they are:

- Only stored on secure shared access drives;
- Easy to access when required;
- Retained in accordance with the relevant record retention policy, i.e. not kept for any longer than necessary.

c. Transportation of files

Great care must be taken when taking paper or digital files out of the office (for example for use in meetings).

- Paper files should be transported securely, especially if they contain personal or sensitive data, and only if absolutely necessary.

Using or storing digital files on or in a physical, moveable source, for example a USB stick or a laptop, should also only be done when absolutely necessary and there are no other, more secure alternatives. Such devices must have:

- Appropriate security, i.e. password protected and with all appropriate virus and other protection;
- All documents on said devices secured with encryption, password protection, etc.

In the event of a paper file or portable device being lost or stolen while in transport, this should be treated as a data breach and reported as such (see section g., Reporting Data Breaches).

d. Paper filing

Where possible, paper documents should be scanned and stored in digital format. Originals should then be securely destroyed. Effort should be made to reduce the amount of paper used and stored on an ongoing basis.

Where it is not possible to scan and store digitally, paper documents should be:

- Stored in a locked / restricted access area;
- Agreed protocols should be in place for filing / cataloguing documents;
- Easy to access when required;
- Retained in accordance with the relevant record retention policy, i.e. not kept for longer than necessary and;
- Once no longer required, documents should be securely destroyed;
- Storage locations should be audited (at least) annually.

e. Emails

- Any email from, or relating to, a student which is received in a personal email account should be moved to an appropriate shared email account's inbox.
- When emailing, think carefully about any information you put down in writing – would you be happy for the person concerned to read it? All information about a person is potentially disclosable to them, via Subject Access Request.
- If you are forwarding an email trail, carefully consider the recipients and whether everything in the included trail is appropriate to be shared with all parties.
- If emailing groups of people, especially when it may be about sensitive information, think carefully about whether you should use BCC rather than CC, or set up email groups / maillists.

- If you receive an email containing information which should not have been sent to you, it is your responsibility to demonstrate best practice by taking the following action;
    - If the underlying email trail contains sensitive information which you have no need to see, respond to the sender, deleting the sensitive information and replacing it with ***This information has been deleted for Data Protection purposes***, and in your email explain to them why you have done this. For example, *"I have deleted the below information since it contains sensitive details about a student's medical history which I have no need to see"*. Also cc data.breach@admin.ox.ac.uk into your response so that the Compliance Team can monitor the number of these occurrences, and forward them the original email so they can see the full details of the breach. Once you have done this, delete the original email.
    - If you are unsure of what should be redacted, or whether or not to redact something, consult your line manager.
    - If the email contains an attachment or other data which you feel has been sent to you in error or which has not been sent via a secure means, respond to the sender and highlight this, suggesting that in future they use a different method of sharing information, as detailed in section e., sharing student information. It may be appropriate to share this document with them to highlight best practice. Also cc data.breach@admin.ox.ac.uk into your response so that the Compliance Team can monitor the number of these occurrences, and forward them the original email so they can see the full details of the breach. Once you have done this, delete the original email.

- If you have accidentally sent an email containing student data to the wrong recipient, report this to your line manager who will advise you on the appropriate action to take (see Reporting Data Breaches below).

f. Sharing Student Information

Reports or other documents containing sensitive student data*, e.g. spreadsheets, must be transmitted securely, by the following method (in order of preference):

- Stored on a secure shared access drive, with a hyperlink sent to share location;
- Shared via SharePoint/OneDrive/Nexus 365/Teams through the production of a secure link, with access given only to those who need to see it, requiring the recipient to access the file through their Single Sign On;
- Password-protected and encrypted when sent by email.

Any files produced for sharing student data should be deleted once they no longer serve a purpose, in accordance with the Student Record Retention Policy.

*Sensitive student data includes (but is not limited to): ethnicity, disability, religious belief, sexual orientation, medical background. Non-sensitive student data includes (but is not limited to): student number, name, course, college. Whilst some data is not formally classified as sensitive, it should still be treated carefully and in the same way as sensitive data. Examples include student results and contact details. If you are uncertain of whether the data you wish to share should be classified as sensitive, contact your line manager.

You should not use OxFile to share student data; this is not a secure file sharing service:

- Links generated do not require the use of Single Sign On to access files;
- In the vast majority of cases emails sent to users containing the URL to access a folder are transferred over the internet with no encryption;
- There is nothing to stop people forwarding an email link onto others who could then also access the file.

g. Reporting Data Breaches

The University must report a breach of personal data to the Information Commissioner's Office (ICO) within 72 hours. If the University fails to report the breach within this given timeframe it could be liable for a significant financial penalty (4% of global annual turnover or €20 million). Where there is a breach of personal data it is essential therefore to take prompt action and immediately report the breach to your line manager and/or head of section.